Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Saturday, December 27, 2008

Bit gold

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party.

Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function.". The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.

Here are the main steps of the bit gold system that I envision:

(1) A public string of bits, the "challenge string," is created (see step 5).

(2) Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

(3) The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

(4) Alice adds the challenge string and the timestamped proof of work string to a distributed property title registryfor bit gold. Here,

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

too, no single server is substantially relied on to properly operate the registry.

(5) The last-created string of bit gold provides the challenge bits for the next-created string.

(6) To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

(7) To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp.

Note that Alice's control over her bit gold does not depend on her sole possession of the bits, but rather on her lead position in the unforgeable chain of title (chain of digital signatures) in the title registry.

All of this can be automated by software. The main limits to the security of the scheme are how well trust can be distributed in steps (3) and (4), and the problem of machine architecture which will be discussed below.

Hal Finney has implemented a variant of bit gold called RPOW (Reusable Proofs of Work). This relies on publishing the computer code for the "mint," which runs on a remote tamper-evident computer. The purchaser of of bit gold can then use remote attestation, which Finney calls the transparent server technique, to verify that a particular number of cycles were actually performed.

The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." (I wrote about this obscurely several years ago.) Thus, it might be possible to be a very low cost producer (by several orders of magnitude) and swamp the market with bit gold. However, since bit gold is timestamped, the time created as well as the mathematical difficulty of the work can be automatically proven. From this, it can usually be inferred what the cost of producing during that time period was.

Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items. In this respect "bit gold" acts more like collector's items than like gold. However, the match between this ex post market and the auction determining the initial value might create a very substantial profit for the "bit gold miner" who invents and deploys an optimized computer architecture.

Thus, bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today to make commodity markets possible. Trust is still distributed because the estimated values of such bundles can be independently verified by many other parties in a largely or entirely automated fashion.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. The potential for initially hidden supply gluts due to hidden innovations in machine architecture is a potential flaw in bit gold, or at least an imperfection which the initial auctions and ex post exchanges of bit gold will have to address.

Posted by Nick Szabo at 4:16 PM

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ▼ 2008 (55)
  - ▼ December (2)
    - Bit gold markets
    - Bit gold
  - ► October (2)
  - ► September (4)
  - ► August (9)
  - ► July (4)
  - ► June (6)
  - ► May (6)
  - ► April (4)
  - ► March (10)
  - ► February (5)
  - ► January (3)
- ► 2007 (47)
- ► 2006 (130)
- ► 2005 (44)

33 comments:

Kay Bell said...

Nick,
This isn't really a comment on this post, but since I haven't found a way to e-mail you, I thought I would use this way to let you know that I referenced one of your papers in a recent entry on my tax blog, Don't Mess With Taxes. It's in the entry about property taxes.
Best,
Kay Bell

2:16 PM

Nick Szabo said...

Thanks! That's a good article you have about property taxes, and it's fascinating to see that narrow houses made it to Virginia.. Here's my cited article on value measurement and taxes.

2:44 PM

Kay Bell said...

I just added the article link in my post. thanks!

3:13 PM

Patrick said...

Hi Nick,
The "Bit Gold" of greatest interest is the string of bits that adds up to valuable new information. The effort involved in calculating a hash value is significant, but the really important effort is that involved in creating something like a substantive contribution to the Linux kernel, or a scientific paper describing original research. The previously unknown bit stream that describes a protein that cures cancer is REAL bit gold, no?

The work that I'm doing at http://infoeng.sourceforge.net is designed to create digital financial instruments that represent such bit streams (that is, software and other useful information).

Sorry for the marketing blurb, and an incomplete blurb at that, but I thought this would be appropriate. :)

Patrick

8:53 PM

theantirobot said...

Would this be the currency of an information economy? I imagine a user produced content site awarding bitgold to users who made popular content, or perhaps promoted content early on which became popular. The website earns revenue, buys gold and puts it in a treasury. Then users can trade in their bitgold for real gold. The site can manipulate/maintain the exchange rate by issuing more bitgold. I imagine that this is the way the government will function in a few years, when the Internet is the government.

8:18 PM

Daniel A. Nagy said...

I have two problems with bitgold:

0.) What makes it desirable? Why would I want to own proofs of wasted computational effort? Gold is desired for various evolutionary reasons on the level of instincts, at least with some people. But meaningless bits? I can't see how bitgold bootstraps into becoming money.

1.) How exact is Moore's law? What is the exchange rate between a gigacycle today and a gigacycle next year?

4:20 PM

Anonymous said...

I somewhat concur with "Daniel A. Nagy's" point #0.

You keep saying that such-and-so "will" happen. That must require some overgeneralization of a principle (monetary standards are based on scarce things) when you haven't explained why or how a "bit gold" standard of money is even
likely to be adopted *out of all the possible alternatives*.

Hypothetically, one might hope that *someone* can be motivated to adopt or promote the standard if a "bit gold" system can be constructed such that the production of "bit gold" performs work of actual value to some party that would thereby be motivated to support the standard. (Not that you ever alluded to this point.)
Examples of useful (if possibly inadequate) work might include any of the tasks that are presently performed by voluntary distributed computing, such as SETI and biochemical analysis.

Nevertheless, I doubt that powerful governments and central banks would be eager to promote or even permit a switchover to a "bit gold" standard when such would demolish much of their present ability to influence the economy through monetary policy.

Anyway, if you read down this far, please understand that you've written much that I admire, and this case is a relatively rare exception.

--Cat Typing Person

8:50 PM

Anonymous said...

I think, a database containing every individuals DNA, generate a private/public key.

When a human is born, that humans DNA goes into the "Bank" and that human is assigned 1 "specialdollar" to be used during their life time, in exchange for goods or services.

So, for example to purchase a loaf of bread would be 0.00000648 "specialdollar" since 365 * 80 / 2 = 14600 (1 loaf of bread every 2 days).

To do the exchange, sign the amount with your bank and generate a note of that amount with your public key.

To prevent inflation, the "Bank" can deduct a percentage from each bank account whenever an individual dies.

This sounds crazy, but with todays technoloy something like this is possible, but boring.

5:07 AM

Jack Lloyd said...

"Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items."

I'm not convinced that this distinction is actually correct. It is just the case that, within the last few centuries, the amount of newly available gold in any year as a percentage of the total stock has been relatively small, so we do not observe this effect. However in Spain in the 1500s the amount of gold imported from the new world was sufficient to cause noticeable inflation.

As an intellectual exercise, consider what would happen to the price of gold if every day each person in the world woke up with a shiny new kruggerand underneath their pillow.

6:15 PM

chaord said...

I know this is an old post, but if you are still interested in proof-of-work systems and their applicability as a digital currency, you might want to check out http://www.bitcoin.org It's a decentralized, P2P, cryptocurrency based on a proof of work algorithm.

12:09 AM

Synonymous said...

Money, in general terms is a limiting factor to the advancement of human civilization.

With your idea, anyone with a computer has the capacity to create wealth! It has much the same business model as land, anyone with land can live form it in various ways.

Your idea puts the power of wealth in the hands of the common people. I hope it catches on!

7:14 AM

Tommy J said...

I agree, this does sound like a revolutionary concept, and I hope it go out.....at least in trial form.

6:02 AM

Anonymous said...

Hi Nick,

Great article! I'm a producer at HuffPost Live, The Huffington Post's online streaming news network. I'm working a web-chat, scheduled for today, Tues. 2/12 at 5pm ET about Bitcoins. Will virtual currency reign in the future? Amazon now has 'coins,' and Bitcoin is preparing for a future dependent on virtual currency. Can cryptography be used to avoid the pitfalls of central authority?

I'd love to hear your thoughts on this topic. Please let me know if you are interested and available to join us via webcam and I will send you further details.

Best,
Shelley Thomas
shelley.thomas@huffingtonpost.com
live.huffingtonpost.com

7:04 AM

Anonymous said...

Congrats on inventing BitCoin

10:04 PM

Anonymous said...

o.m.agunloye@gmail.com

I like this idea, but what I don't agree with is the centralization. Bitcoin is already on that, so why don't you implement this with...well email me to find out my thoughts (if you care).

8:47 AM

Anonymous said...

Thanks for laying the foundation for bitcoin Nick, we owe a great debt to you.

8:40 PM

algroista said...

Here is the record of a great moment in human history.

11:40 AM

Sebastian Schepis said...

One day, people will look upon this post as the actual genesis moment of Bitcoin. This is a a piece of digital history, worthy of preservation. Thank you Nick.

8:23 AM

Sandro said...

It's a pleasure to leave my minuscule sign in this fundamental page for the history of mankind.

5:58 PM

jessilydia said...

It's very *odd* that such smart people miss the basic problem left unsolved. No matter what the token, its value is what you can exchange it for.

The real threat to the stability of currencies has been the self-contradictory *practice* (whatever coinage is used) of compounding returns on investment, as if believing that every coin earned in the past can be owed limitlessly growing new returns in the future.

Yes, I know the idea of investors having the responsibility to **spend their winnings**, as the one way to keep debts in the system from becoming an existential threat to the system, and destabilizing the pool, is just silly and abhorrent to money makers as anything

could be. It's also VERY REAL OBLIGATION TO PRESERVE THE SYSTEM, in environmental terms.

No matter what pile of credit you accumulate, it's ONLY real value is what you can EXCHANGE IT FOR. So accumulating credits for SERVICES NOT CONSUMED, withdrawing the credit to your own account exponentially, and so removing it from the system for exchanges as a rule, as we're all told to do to "make money", doesn't work.

It does in fact directly cause what you can exchange it for to inflate in false value to a point of collapse, *very naturally*.

4:51 AM

Anonymous said...

Here lies something beautiful. Polymatheus

8:53 AM

PeterIII said...

Well said Sandro.

Thank you Nick.

12:47 PM

Tom Eck said...

Mssr. Szabo, the entire cryptocurrency 'establishment' owes you an immense debt of gratitude. I do agree with some of the comments (and had arrived at the same opinion independently) that we'd be better off with a POW function that does something more important than just solving a meaningless puzzle. I'm thinking of a domain-specific function such as predicting protein folding (critical in medicine and bio-tech) or for general purpose (e.g. spending cycles on a highly distributed problem, which has its own value). Of course, the two major constraints of POW must be maintained: 1/ confirmation of the solution must be trivial, and 2/ the computational cost for producing the solution must be controllable. Or maybe not - perhaps you get more in return for having provided more value in your POW.

4:23 PM

Jonathan James Harrison said...

Thank you soo much Nick, your thinking has changed my life in nearly every aspect. Much love and respect.

6:10 PM

Anonymous said...

great idea that will revolutionize the way we do business. its now 2015... only a couple of more years and I believe it will be a mainstream thing. Congratulations on your good work.

Deno

7:05 AM

Anonymous said...

One small post for Nick, a giant leap for humanity.
Simply Nobel prise worthy.
MG

7:09 PM

Raymond Blanchard said...

You changed many a nerds life

3:45 AM

Matthew said...

And thus the world is changed, forever, for the better.

Thanks Nick

7:56 PM

zac said...

Interesting to think of the (cost of work)/coin as the fundamental price-driving force. Makes me wonder what will happen to the price of other coins when the rewards halve, or the even more unknown territory, proof-of-steak

4:26 PM

Nosliv said...

Inspiring...

Freedom is never given; it is won.

8:26 AM

Anonymous said...

Nick I hope this concept becomes every mans reality :)

9:48 PM

Alex Millar (@bitcoin3000) said...

Nick, amazing work. Thank you. That you foresaw the issue of ASIC's is demonstrates your great knowledge: "The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." "

2:17 PM

Charles said...

RESPECT SIR! Thank you for everything you've done NS.

6:49 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.